

## PATENT ABSTRACTS OF JAPAN

W1505

(11)Publication number : 2003-016418

(43)Date of publication of application : 17.01.2003

(51)Int.Cl.

G06K 19/10

B42D 15/10

G06F 12/00

G06F 12/14

G06K 19/07

(21)Application number : 2001-194749

(71)Applicant : SONY CORP

(22)Date of filing : 27.06.2001

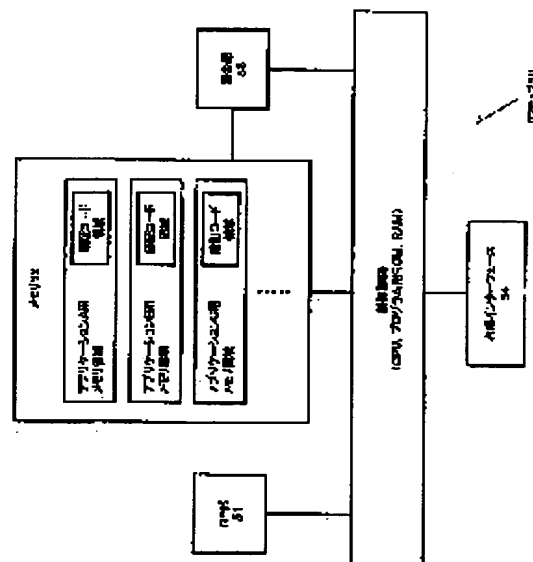
(72)Inventor : YAMAGATA AKIHIKO  
FUKADA AKIRA

(54) PORTABLE TERMINAL AND ITS CONTROL METHOD, AND IC CARD

(57)Abstract:

PROBLEM TO BE SOLVED: To efficiently control the right to access each application allocated to a memory area of an IC card.

SOLUTION: By introducing a hierarchical structure to memory areas on the IC card, respective applications allocated to the memory areas are registered in directories, and the memory areas are managed by directories. Password codes are set for every application and directory and the right to access is controlled in the application units and directory units. If a portable terminal is lost, the right to access the applications in the IC card is automatically lost.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

W1508

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-16418

(P2003-16418A)

(43) 公開日 平成15年1月17日 (2003.1.17)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
G 0 6 K 19/10		B 4 2 D 15/10	5 2 1 2 C 0 0 5
B 4 2 D 15/10	5 2 1	G 0 6 F 12/00	5 3 7 D 5 B 0 1 7
G 0 6 F 12/00	5 3 7	12/14	3 2 0 C 5 B 0 3 5
12/14	3 2 0	G 0 6 K 19/00	R 5 B 0 8 2
G 0 6 K 19/07			H

審査請求 未請求 請求項の数18 O L (全 17 頁)

(21) 出願番号 特願2001-194749 (P2001-194749)

(22) 出願日 平成13年6月27日 (2001.6.27)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 山形 昭彦

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 深田 顕

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100101801

弁理士 山田 英治 (外2名)

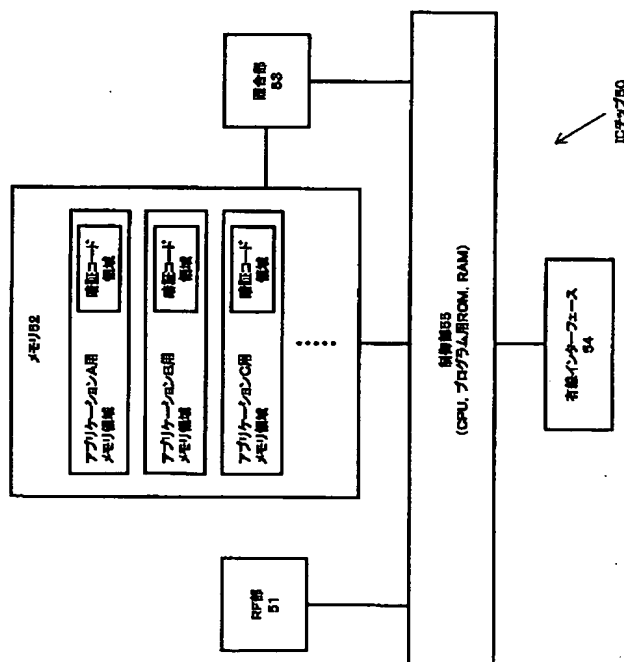
最終頁に続く

(54) 【発明の名称】 携帯端末及びその制御方法、並びに、I Cカード

(57) 【要約】

【課題】 I Cカードのメモリ領域に割り当てられた各アプリケーションへのアクセス権を効率的に制御する。

【解決手段】 I Cカード上のメモリ領域に階層構造を導入することにより、メモリ領域上に割り当てられた各アプリケーションをディレクトリに登録して、ディレクトリ毎にメモリ領域を管理する。アプリケーション毎、並びにディレクトリ毎に暗証コードを設定して、アプリケーション単位又はディレクトリ単位でアクセス権を制御する。また、携帯端末を紛失した場合には、I Cカード内のアプリケーションへのアクセス権が自動的に消失する。



## 【特許請求の範囲】

【請求項 1】外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えた IC チップを搭載した携帯端末であって、

前記 IC チップ上のメモリ領域に割り当てられた、暗証コードによりアクセス権が制御された 1 以上のアプリケーションと、

前記 IC チップが外部機器と無線通信するための無線インターフェースと、

前記携帯端末内で前記 IC チップと有線通信するための有線インターフェースと、

ユーザが暗証コードその他のデータを入力することができるユーザ入力手段と、

前記ユーザ入力手段から入力された暗証コード前記有線インターフェースを介して前記 IC チップに転送して、前記 IC チップ上のメモリ領域に割り当てられた各アプリケーションの暗証コードと比較照合する照合手段と、前記照合手段による比較照合の結果、暗証コードが一致するアプリケーションに関するアクセス権をユーザに与えるアクセス権制御手段と、を具備することを特徴とする携帯端末。

【請求項 2】前記アクセス権制御手段は、アクセス権が与えられたアプリケーションに対する外部機器からの前記無線インターフェースを介した無線通信によるアクセスを許容する、ことを特徴とする請求項 1 に記載の携帯端末。

【請求項 3】前記アクセス権制御手段は、前記無線インターフェース経由で接続された外部機器からの電波を検出しなくなったことに応答して、アクセス権を付与したアプリケーションに関する一連のトランザクションが終了したと判断して、トランザクション終了処理を行なう、ことを特徴とする請求項 1 に記載の携帯端末。

【請求項 4】前記アクセス権制御手段は、前記 IC チップから前記無線インターフェース経由で送出したコマンドに対するレスポンスが所定時間内に受信されなかったことに応答して、前記無線インターフェース経由で接続された外部機器と前記 IC チップとの一連のトランザクションが正常又は異常終了したとみなして、終了処理を行なう、ことを特徴とする請求項 1 に記載の携帯端末。

【請求項 5】アプリケーション毎にあらかじめ暗証コードを登録する暗証コード登録手段と、

プログラム起動手段と、

起動されたプログラムに応じて該当するアプリケーションに対応する暗証コードを前記有線インターフェース経由で前記 IC チップに入力する暗証コード入力手段と、をさらに備えることを特徴とする請求項 1 に記載の携帯端末。

【請求項 6】前記 IC チップは、

前記無線インターフェース経由で外部機器に接続されて給電されたことに応答して、前記 IC チップ上のメモリ

領域にアクセスするために暗証コードの入力が必要である旨を前記有線インターフェース経由で通知する、ことを特徴とする請求項 1 に記載の携帯端末。

【請求項 7】外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えた IC チップを搭載した携帯端末の制御方法であって、

前記携帯端末は、前記 IC チップが外部機器と無線通信するための無線インターフェースと、前記携帯端末内で前記 IC チップと有線通信するための有線インターフェースとを備え、

前記 IC チップ上のメモリ領域には暗証コードによりアクセス権が制御された 1 以上のアプリケーションが割り当てられており、

ユーザから暗証コードを入力するユーザ入力ステップと、

前記ユーザ入力ステップにより入力された暗証コードを前記有線インターフェース経由で前記 IC チップに送出するステップと、

前記 IC チップ上のメモリ領域に割り当てられた各アプリケーションの暗証コードと、前記ユーザ入力ステップにより入力された暗証コードとを比較照合する照合ステップと、

前記照合ステップにおける比較照合の結果、暗証コードが一致するアプリケーションに関するアクセス権をユーザに与えるアクセス権制御ステップと、を具備することを特徴とする携帯端末の制御方法。

【請求項 8】前記アクセス権制御ステップでは、アクセス権が与えられたアプリケーションに対する外部機器からの前記無線インターフェースを介した無線通信によるアクセスを許容する、ことを特徴とする請求項 7 に記載の携帯端末の制御方法。

【請求項 9】前記アクセス権制御ステップでは、前記無線インターフェース経由で接続された外部機器からの電波を検出しなくなったことに応答して、アクセス権を付与したアプリケーションに関する一連のトランザクションが終了したと判断して、トランザクション終了処理を行なう、ことを特徴とする請求項 7 に記載の携帯端末の制御方法。

【請求項 10】前記アクセス権制御ステップでは、前記 IC チップから前記無線インターフェース経由で送出したコマンドに対するレスポンスが所定時間内に受信されなかったことに応答して、前記無線インターフェース経由で接続された外部機器と前記 IC チップとの一連のトランザクションが正常又は異常終了したとみなして、終了処理を行う、ことを特徴とする請求項 7 に記載の携帯端末の制御方法。

【請求項 11】アプリケーション毎にあらかじめ暗証コードを登録する暗証コード登録ステップと、

プログラム起動ステップと、

起動されたプログラムに応じて該当するアプリケーショ

ンに対応する暗証コードを前記有線インターフェース経由で前記ICチップに入力する暗証コード入力ステップと、をさらに備えることを特徴とする請求項7に記載の携帯端末の制御方法。

【請求項12】前記ICチップが前記無線インターフェース経由で外部機器に接続されて給電されたことに応答して、前記ICチップ上のメモリ領域にアクセスするために暗証コードの入力が必要である旨を前記有線インターフェース経由で通知するステップをさらに備える、ことを特徴とする請求項7に記載の携帯端末の制御方法。

【請求項13】携帯端末に付随して使用されるICカードであって、

外部機器と無線通信するための無線インターフェースと、  
前記携帯端末と有線通信するための有線インターフェースと、

暗証コードによりアクセス権が制御された1以上のアプリケーションが割り当てられたメモリ領域と、を具備し、前記無線インターフェース経由で外部機器に接続されたことに応答して給電されて駆動する、ことを特徴とするICカード。

【請求項14】前記無線インターフェース経由で受信した暗証コードが一致したことに応答して、メモリ領域上の対応するアプリケーションのアクセス権が前記無線インターフェース経由で接続された外部機器に与えられる、ことを特徴とする請求項13に記載のICカード。

【請求項15】前記有線インターフェース経由で受信した暗証コードが一致したことに応答して、メモリ領域上の対応するアプリケーションのアクセス権が前記無線インターフェース経由で接続された外部機器に与えられる、ことを特徴とする請求項13に記載のICカード。

【請求項16】前記無線インターフェース経由で接続された外部機器からの電波を検出しなくなったことに応答して、該外部機器に与えられているアプリケーションへのアクセス権が失効する、ことを特徴とする請求項13に記載のICカード。

【請求項17】前記無線インターフェース経由で送出したコマンドに対するレスポンスが所定時間内に受信されなかったことに応答して、該外部機器に与えられているアプリケーションへのアクセス権が失効する、ことを特徴とする請求項13に記載のICカード。

【請求項18】前記無線インターフェース経由で外部機器に接続されて給電されて駆動することに応答して、前記ICチップ上のメモリ領域にアクセスするために暗証コードの入力が必要である旨を前記有線インターフェース経由で通知する、ことを特徴とする請求項13に記載のICカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、外部機器との無線

通信により給電されて駆動するICチップを搭載した携帯端末、並びに、携帯端末に付随して使用されるICカードに係り、特に、外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたICチップを搭載した携帯端末及びその制御方法、並びに、メモリ機能を備えたICカードに関する。

【0002】更に詳しくは、本発明は、ICチップ上のメモリ領域に1以上のアプリケーションが割り当てられた携帯端末及びその制御方法、並びに、メモリ領域に1以上のアプリケーションが割り当てたICカードに係り、特に、ICチップ上のメモリ領域に割り当てられた各アプリケーション毎にアクセス権を制御する携帯端末及びその制御方法、並びに、メモリ領域に割り当てられた各アプリケーション毎にアクセス権を制御するICカードに関する。

【0003】

【従来の技術】従来から、本人確認や認証処理のために暗証番号やパスワードを用いたさまざまな装置が考案され、実用に供されている。（ここで、一般に、「暗証番号」とは0から9までの数字の組み合わせで表される文字列のことを言い、また、「パスワード」は、数字に加えてアルファベットなどの一般文字を用いて表される文字列のことを言う。本明細書中では、暗証番号とパスワードを併せて「暗証コード」とも呼ぶ。）

【0004】例えば、銀行やその他の金融機関において、キャッシュカードを使用する際には、キャッシュ・ディスペンサなどで、本人認証の手段として、暗証番号やパスワードの入力を使用者に対して促し、使用者から正しい暗証番号やパスワードが入力されたことを確認してから、キャッシュ・ディスペンサなどから出金動作を行なうようになっている。

【0005】この他にも、ホテルなどの宿泊施設に設置されたセーフティ・ボックスの暗証コード入力、コンピュータへのログイン時のパスワード入力、あるいは情報端末上の情報を秘匿するためなど、暗証コードに関する適用例はさまざまである。

【0006】従来、1枚の銀行用キャッシュカード上に配設されている磁気ストライプなどの記憶媒体の中には、その銀行に対してのみ使用可能な記憶領域しか設けられていない。したがって、上述したような暗証番号あるいはパスワードの入力は、この単一の記憶領域へのアクセスに過ぎない。したがって、ユーザは、目的又は用途毎にカードを用意して、複数のカードを使い分ける必要がある。

【0007】最近では、非接触方式のICカードが普及してきている。例えばキャッシュ・ディスペンサやコンサート会場の出入口、駅の改札口などに設置されたICカード・リーダ／ライタは、利用者がかざしたICカードに非接触でアクセスすることができる。ここで、利用者が暗証番号やパスワードをICカード・リーダ側に入

力して、入力された暗証番号やパスワードをICカード上に格納された暗証番号やパスワードと照合することで、ICカードとICカード・リーダー/ライター間で本人確認又は認証処理が行なわれる。そして、本人確認又は認証処理に成功した場合には、例えば、ICカード内に保存されているアプリケーションの利用が可能となる。ここで、ICカードが保持するアプリケーションとしては、例えば、電子マネーや電子チケットなどの価値情報を挙げることができる。

【0008】また、最近では、微細化技術の向上とも相俟って、比較的大容量の記憶空間を持つICカードが出現し、普及してきている。従来のキャッシュ・カードなどにおいては単一の記憶領域すなわち単一のアプリケーションしか担持しないので、各用途又は目的毎に応じた複数のカードを持ち歩く必要ができる。これに対して、このような大容量メモリ付きのICカードによれば、複数のアプリケーションを同時に格納しておくことができるので、1枚のICカードを複数の用途に利用することができる。例えば、1枚のICカード上に、電子決済を行なうための電子マネーや、特定のコンサート会場に入場するための電子チケットなど、2以上のアプリケーションを格納しておき、1枚のICカードをさまざまな用途に適用させることができる。

【0009】さらに、このような大容量メモリ機能付きのICカード（又は、ICカード機能が半導体チップ化されたICチップ）を、携帯電話機などの携帯端末上に搭載することによって、利用者は携帯端末を所持しておくことで、電子決済を始めとする外部との電子的な価値情報のやり取りを行なうことができる。

【0010】従来のキャッシュ・カードは単一の用途しか持たないので（前述）、キャッシュ・カード上の磁気ストライプは単一の暗証番号又はパスワードを持つことによってカード全体のセキュリティを管理することができた。

【0011】これに対し、複数のアプリケーションを保持することができるメモリ機能付きICカードや、このようなICカード（又はICチップ）を搭載した携帯端末においては、アプリケーション毎にアクセス権を制御する必要がある。何故ならば、唯1つの暗証コードのみで、ICカード上のすべてのアプリケーションへのアクセスを開放してしまうと、例えば紛失時や盗難時におけるセキュリティが著しく低下するからである。

【0012】

【発明が解決しようとする課題】本発明の目的は、外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたICチップを搭載した優れた携帯端末及びその制御方法、並びに、メモリ機能を備えた優れたICカードを提供することにある。

【0013】本発明の更なる目的は、ICチップ上のメモリ領域に1以上のアプリケーションが割り当てられた

優れた携帯端末及びその制御方法、並びに、メモリ領域に1以上のアプリケーションが割り当てた優れたICカードを提供することにある。

【0014】本発明の更なる目的は、ICチップ上のメモリ領域に割り当てられた各アプリケーション毎にアクセス権を制御することができる、優れた携帯端末及びその制御方法、並びに、メモリ領域に割り当てられた各アプリケーション毎にアクセス権を制御することができる優れたICカードを提供することにある。

【0015】

【課題を解決するための手段及び作用】本発明は、上記課題を参酌してなされたものであり、その第1の側面は、外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたICチップを搭載した携帯端末であって、前記ICチップ上のメモリ領域に割り当てられた、暗証コードによりアクセス権が制御された1以上のアプリケーションと、前記ICチップが外部機器と無線通信するための無線インターフェースと、前記携帯端末内で前記ICチップと有線通信するための有線インターフェースと、ユーザが暗証コードやその他のデータを入力することができるユーザ入力手段と、前記ユーザ入力手段から入力された暗証コード前記有線インターフェースを介して前記ICチップに転送して、前記ICチップ上のメモリ領域に割り当てられた各アプリケーションの暗証コードと比較照合する照合手段と、前記照合手段による比較照合の結果、暗証コードが一致するアプリケーションに関するアクセス権をユーザに与えるアクセス権制御手段と、を具備することを特徴とする携帯端末である。

【0016】ここで言う携帯端末とは、例えば、携帯電話機や、PDA（Personal Digital Assistant）などのような、小型且つ軽量に構成されて、ユーザが絶えず持ち歩くことができる情報処理装置のことを指す。

【0017】ICチップにアンテナを搭載してクレジットカード・サイズ大に構成されたカートリッジのことを、一般に、「ICカード」と呼ばれる。ICチップは、携帯電話機やPDAなどの携帯端末や、その他の情報処理装置に内蔵して用いられる。また、ICカードを情報処理装置に挿入して使用することもある。ICチップ若しくはICカードの使用形態としては、プリペイド形式の電子マネーや電子チケットなどの価値情報に関する機能が挙げられる。ICチップ又はICカードによって提供される機能のことを、以下では、「アプリケーション」とも呼ばれる。

【0018】本発明の第1の側面に係る携帯端末上に搭載されたICチップは、リーダー/ライターなどの外部機器と無線接続するための無線インターフェースと、搭載された携帯端末側のコントローラなどと内部接続するための有線インターフェースを備えており、リーダー/ライターと無線接続されたことに応答して、其処から届く電波に

より駆動可能となる。

【0019】また、本発明の第1の側面に係る携帯端末上に搭載されたICチップは、比較的大容量メモリのメモリ領域を備えている。このメモリ領域上には、1以上のアプリケーションが割り当てられている。各アプリケーションのアクセス権は、暗証番号やパスワードなどの暗証コードによって制御される。ここで言うアプリケーションには、電子マネーや電子チケットなどの価値情報が含まれる。

【0020】リーダ/ライタなどの外部機器に無線接続した状態では、リーダ/ライタ上で入力された暗証コードが無線インターフェースでICチップに入力することができる。また、携帯端末上のキーボードなどのユーザ入力装置上から入力された暗証コードは、有線インターフェース経由でICチップに入力することができる。そして、無線インターフェース又は有線インターフェースから入力された暗証コードを比較照合して、その一致により、該当するアプリケーションへのアクセス権が与えられる。

【0021】本発明の第1の側面によれば、まず、携帯端末上で所望のアプリケーションの暗証コードを入力しておいてから、リーダ/ライタのような外部機器に携帯端末をかざすことによって、そのまま外部機器上でアプリケーションを使用する（例えば、電子決済を行なう）ことができる。したがって、ユーザは、操作が不慣れた外部機器上のユーザ・インターフェースではなく、操作が手慣れた自分の携帯端末上で暗証コードを入力操作して、照合処理を受けることができる。すなわち、ICチップを内蔵した情報処理機器上で暗証コードを入力してロックを解除後に外部機器と無線接続して、メモリ領域へのアクセスを許容するようにしてもよい。勿論、情報処理機器内のICチップと外部機器との無線接続を確立した後、外部機器上で入力される暗証コードを基にアクセス権を制御するようにしてもよい。

【0022】前記アクセス権制御手段は、アクセス権が与えられたアプリケーションに対する外部機器からの前記無線インターフェースを介した無線通信によるアクセスを許容するようにしてもよい。

【0023】また、前記アクセス権制御手段は、前記無線インターフェース経由で接続された外部機器からの電波を検出しなくなったことに応答して、アクセス権を付与したアプリケーションに関する一連のトランザクションが終了したと判断して、トランザクション終了処理を行なうようにしてもよい。したがって、使用後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【0024】また、前記アクセス権制御手段は、前記IC

Cチップから前記無線インターフェース経由で送出したコマンドに対するレスポンスが所定時間内に受信されなかったことに応答して、前記無線インターフェース経由で接続された外部機器と前記ICチップとの一連のトランザクションが正常又は異常終了したとみなして、終了処理を行なうようにしてもよい。したがって、外部機器との無線接続が断たれた後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【0025】本発明の第1の側面に係る携帯端末は、アプリケーション毎にあらかじめ暗証コードを登録する暗証コード登録手段と、プログラム起動手段と、起動されたプログラムに応じて該当するアプリケーションに対応する暗証コードを前記有線インターフェース経由で前記ICチップに入力する暗証コード入力手段とをさらに備えていてもよい。このような場合、ユーザがディスプレイに表示されたメニュー画面などを介して所望のプログラムを選択して、携帯端末上で該当するプログラムが呼び出される。そして、起動されたプログラムに応答して、対応するアプリケーションについての暗証コードが前記有線インターフェース経由でICチップに入力されてアクセス権を与えることができる。したがって、ユーザは、使用したいアプリケーションの暗証コードを入力する作業を省略することができ、操作性が向上する。

【0026】また、前記ICチップは、前記無線インターフェース経由で外部機器に接続されて給電されたことに応答して、前記ICチップ上のメモリ領域にアクセスするために暗証コードの入力が必要である旨を前記有線インターフェース経由で通知するようにしてもよい。ICチップを搭載した携帯端末上では、この通知に応答して、ディスプレイ上にダイアログを出現させたり、警告音を発して、ユーザに知らせることができる。したがって、ユーザは、携帯端末をリーダ/ライタなどの外部機器にかざしてアプリケーションを利用したいときに、暗証コードを入力する必要があるということを、確実に思い出すことができるので、ユーザの日常生活の各局面においてアプリケーションの使用が円滑化する。

【0027】また、本発明の第2の側面は、外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたICチップを搭載した携帯端末の制御方法であって、前記携帯端末は、前記ICチップが外部機器と無線通信するための無線インターフェースと、前記携帯端末内で前記ICチップと有線通信するための有線インターフェースとを備え、前記ICチップ上のメモリ領域には暗証コードによりアクセス権が制御された1以上のアプリケーションが割り当てられており、ユーザから暗証コードを入力するユーザ入力ステップと、前記ユーザ

入力ステップにより入力された暗証コードを前記有線インターフェース経由で前記 IC チップに送出するステップと、前記 IC チップ上のメモリ領域に割り当てられた各アプリケーションの暗証コードと、前記ユーザ入力ステップにより入力された暗証コードとを比較照合する照合ステップと、前記照合ステップにおける比較照合の結果、暗証コードが一致するアプリケーションに関するアクセス権をユーザに与えるアクセス権制御ステップと、を具備することを特徴とする携帯端末の制御方法である。

【0028】本発明の第2の側面に係る携帯端末上に搭載された IC チップは、リーダ/ライタなどの外部機器と無線接続するための無線インターフェースと、搭載された携帯端末側のコントローラなどと内部接続するための有線インターフェースを備えており、リーダ/ライタと無線接続されたことに応答して、その電波により駆動可能となる。

【0029】また、本発明の第2の側面に係る携帯端末上に搭載された IC チップは、比較的大容量メモリのメモリ領域を備えている。このメモリ領域上には、1以上のアプリケーションが割り当てられている。各アプリケーションのアクセス権は、暗証番号やパスワードなどの暗証コードによって制御される。ここで言うアプリケーションには、電子マネーや電子チケットなどの価値情報が含まれる。

【0030】リーダ/ライタなどの外部機器に無線接続した状態では、リーダ/ライタ上で入力された暗証コードが無線インターフェースで IC チップに入力することができる。また、携帯端末上のキーボードなどのユーザ入力装置上から入力された暗証コードは、有線インターフェース経由で IC チップに入力することができる。そして、無線インターフェース又は有線インターフェースから入力された暗証コードを比較照合して、その一致により、該当するアプリケーションへのアクセス権が与えられる。

【0031】本発明の第2の側面によれば、まず、携帯端末上で所望のアプリケーションの暗証コードを入力しておいてから、リーダ/ライタのような外部機器に携帯端末をかざすことによって、そのまま外部機器上でアプリケーションを使用する（例えば、電子決済を行なう）ことができる。したがって、ユーザは、操作が不慣れた外部機器上のユーザ・インターフェースではなく、操作が手慣れた自分の携帯端末上で暗証コードを入力操作して、照合処理を受けることができる。

【0032】ここで、前記アクセス権制御ステップでは、アクセス権が与えられたアプリケーションに対する外部機器からの前記無線インターフェースを介した無線通信によるアクセスを許容するようにしてもよい。

【0033】また、前記アクセス権制御ステップでは、前記無線インターフェース経由で接続された外部機器か

らの電波を検出しなくなったことに応答して、アクセス権を付与したアプリケーションに関する一連のトランザクションが終了したと判断して、トランザクション終了処理を行なうようにしてもよい。したがって、使用後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【0034】また、前記アクセス権制御ステップでは、前記 IC チップから前記無線インターフェース経由で送出したコマンドに対するレスポンスが所定時間内に受信されなかったことに応答して、前記無線インターフェース経由で接続された外部機器と前記 IC チップとの一連のトランザクションが正常又は異常終了したとみなして、終了処理を行なうようにしてもよい。したがって、外部機器との無線接続が断たれた後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【0035】本発明の第2の側面に係る携帯端末の制御方法は、アプリケーション毎にあらかじめ暗証コードを登録する暗証コード登録ステップと、プログラム起動手段と、起動されたプログラムに応じて該当するアプリケーションに対応する暗証コードを前記有線インターフェース経由で前記 IC チップに入力する暗証コード入力ステップとをさらに備えていてもよい。このような場合、ユーザがディスプレイに表示されたメニュー画面などを介して所望のプログラムを選択して、携帯端末上で該当するプログラムが呼び出される。そして、起動されたプログラムに応答して、対応するアプリケーションについての暗証コードが前記有線インターフェース経由で IC チップに入力されてアクセス権を与えることができる。このような場合、ユーザは、使用したいアプリケーションの暗証コードを入力する作業を省略することができ、操作性が向上する。

【0036】また、前記 IC チップが前記無線インターフェース経由で外部機器に接続されて給電されたことに応答して、前記 IC チップ上のメモリ領域にアクセスするために暗証コードの入力が必要である旨を前記有線インターフェース経由で通知するステップをさらに備えていてもよい。携帯端末上では、この通知に応答して、ディスプレイ上にダイアログを出現させたり、警告音を発して、ユーザに知らせることができる。したがって、ユーザは、携帯端末をリーダ/ライタなどの外部機器にかざしてアプリケーションを利用したいときに、暗証コードを入力する必要があるということを、確実に思い出す



ことができるので、ユーザの日常生活の各局面においてアプリケーションの使用が円滑化する。

【0037】また、本発明の第3の側面は、携帯端末に付随して使用されるICカードであって、外部機器と無線通信するための無線インターフェースと、前記携帯端末と有線通信するための有線インターフェースと、暗証コードによりアクセス権が制御された1以上のアプリケーションが割り当てられたメモリ領域と、を具備し、前記無線インターフェース経由で外部機器に接続されたことに応答して給電されて駆動する、ことを特徴とするICカードである。

【0038】そして、前記無線インターフェース経由で受信した暗証コードが一致したことに応答して、メモリ領域上の対応するアプリケーションのアクセス権が前記無線インターフェース経由で接続された外部機器に与えられる。

【0039】あるいは、前記有線インターフェース経由で受信した暗証コードが一致したことに応答して、メモリ領域上の対応するアプリケーションのアクセス権が前記無線インターフェース経由で接続された外部機器に与えられる。このような場合、まず、携帯端末上で所望のアプリケーションの暗証コードを入力しておいてから、リーダ／ライタのような外部機器に携帯端末をかざすことによって、そのまま外部機器上でアプリケーションを使用する（例えば、電子決済を行なう）ことができる。したがって、ユーザは、操作が不慣れた外部機器上のユーザ・インターフェースではなく、操作が手慣れた自分の携帯端末上で暗証コードを入力操作して、照合処理を受けることができる。

【0040】本発明の第3の側面に係るICカードは、前記無線インターフェース経由で接続された外部機器からの電波を検出しなくなったことに応答して、該外部機器に与えられているアプリケーションへのアクセス権が失効するようにしてもよい。したがって、使用後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【0041】また、本発明の第3の側面に係るICカードは、前記無線インターフェース経由で送出したコマンドに対するレスポンスが所定時間内に受信されなかったことに応答して、該外部機器に与えられているアプリケーションへのアクセス権が失効するようにしてもよい。したがって、外部機器との無線接続が断たれた後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【0042】また、本発明の第3の側面に係るICカードは、前記無線インターフェース経由で外部機器に接続されて給電されたことに応答して、前記ICチップ上のメモリ領域にアクセスするために暗証コードの入力が必要である旨を前記有線インターフェース経由で通知するようにしてもよい。ICカードが付随する携帯端末上では、この通知に応答して、ディスプレイ上にダイアログを出現させたり、警告音を発して、ユーザに知らせることができる。したがって、ユーザは、携帯端末をリーダ／ライタなどの外部機器にかざしてアプリケーションを利用したいときに、暗証コードを入力する必要があるということを、確実に思い出すことができるので、ユーザの日常生活の各局面においてアプリケーションの使用が円滑化する。

【0043】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0044】

【発明の実施の形態】以下、図面を参照しながら本発明の実施例を詳解する。

【0045】図1には、本発明の一実施形態に係る携帯端末10のハードウェア構成を模式的に示している。携帯端末10は、例えば、携帯電話機やPDA(Personal Digital Assistant)などのような、小型且つ軽量に構成されて、ユーザが常に持ち運ぶことができる情報処理端末である。

【0046】図示の携帯端末10は、外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたICチップ50を搭載するとともに、携帯端末10内の動作を統括的に制御するコントローラ11と、ユーザが暗証番号やパスワードを始めとする各種の文字列やコマンドを入力するためのキー／ボタンなどからなるユーザ入力装置12と、処理結果を画面表示するための液晶ディスプレイ(LCD: liquid Crystal Display)などの表示装置13を備えている。もちろん、携帯端末10としての本来の機能を実現するために、図示する以外の周辺装置や回路コンポーネントを備えていてもよい。

【0047】ここで、ICチップにアンテナを搭載してクレジットカード・サイズ大に構成されたカートリッジのことを、一般に、「ICカード」と呼ばれる。

【0048】また、携帯端末10がICチップ50を装備する形態は一意ではない。例えば、半導体チップの形態のICを無線アンテナとともに内蔵するようにしてもよいし、カード状に構成されたICチップすなわちICカードを、携帯端末10に配設されたカード・スロットなどに挿入して用いるようにしてもよい。ICチップ若しくはICカードの使用形態としては、プリペイド形式の電子マネーや電子チケットなどの価値情報に関する機能が挙げられる。ICチップ又はICカードによって提供される機能のことを、以下では、「アプリケーション

ン」とも呼ぶ。

【0049】コントローラ11は、CPU (Central Processing Unit)、ROM (Read Only Memory)、RAM (Random Access Memory)などを一体化して構成される。コントローラ11は、ROM上に格納されたプログラム・コードを実行することによって、携帯端末10内の各種オペレーションを制御する。

【0050】ICチップ50は、外部機器100と無線接続するための無線インターフェース14と、携帯端末10側のコントローラ11と有線接続するための有線インターフェース15を備えている。無線インターフェース14に関しては、例えば、ISO 7816で定義された接触インターフェース規格、又は、ISO 14443で定義された無線インターフェース規格を使用することができる。ICチップ50と外部機器100との接続方式に関しては、後述に譲る。

【0051】ICチップ50は、例えば、非接触ICカードの技術が適用されており、無線インターフェース14経由で受信される外部機器100からの電波によって駆動する。言い換えれば、ユーザが外部機器100に携帯端末10をかざしていない状態では、外部機器100からの電波が届かなくなり、ICチップ50の動作は減勢されてしまう。本実施形態では、電波が途切れることに応答して、ICチップ50内部へのアクセス権は消失する(後述)。

【0052】また、本実施形態に係るICチップ50は、比較的大容量のメモリ領域を備えている。このようなメモリ領域は、微細化技術などによりもたらされる。メモリ領域は、半導体メモリや磁気ストライプ、あるいは読み書き可能なその他の記憶媒体で構成される。このメモリ領域上には、1以上のアプリケーションが割り当てられている。ここで言うアプリケーションの例としては、電子マネーや電子チケットを始めとする価値情報を挙げることができる。

【0053】この種の価値情報を無断使用や盗用から保護するために、各アプリケーション毎に暗証番号やパスワードなどの暗証コードを設定することによって、アプリケーション単位でメモリ領域へのアクセス権が制御されている。例えば、無線インターフェース14や有線インターフェース15を介して入力された暗証コードと各アプリケーションが持つ暗証コードとを比較照合して、一致するアプリケーションについてのアクセス権が与えられる(後述)。

【0054】外部機器100は、ICチップ50のメモリ領域に割り当てられているアプリケーションを利用する装置であり、例えば非接触ICカードの技術を適用して、ICチップ50と無線接続するためのリーダ/ライタ101を含んでいる。勿論、外部機器100は、それ以外にも、特定業務用の演算処理を行なう回路コンポーネントや周辺装置類、ユーザとの対話入力を行うための

表示装置並びに入力装置(いずれも図示しない)を装備している。

【0055】外部機器100は、例えば、銀行内のATM (Automatic Teller Machine) 端末のような電子マネーを使用する装置や、コンサート会場のゲートや駅や空港の改札口など電子チケットを使用する装置など電子的な価値情報を処理する装置、さらには、宿泊施設のセーフティ・ボックスのように本人確認又は認証処理を行なう装置である。

【0056】図1に示すようなシステム構成によれば、ユーザは携帯端末10上のユーザ入力装置12から暗証コードを入力して、ロックを解除する。場合によってはユーザから入力された値を表示装置13上で確認して、携帯端末10に内蔵されたICチップ50に入力された暗証コードを有線インターフェース15経由で送出する。そして、ICチップ50内では、メモリ領域上の各アプリケーション又は各ディレクトリに設定されている暗証コードとユーザ入力された暗証コードの照合が行なわれる。そして、一致するアプリケーション又はディレクトリに割り当てられたメモリ領域へのアクセス権がユーザに与えられる。あるいは、携帯端末10内のICチップ50と外部機器100との無線接続を確立した後、外部機器100上で入力される暗証コードを基に、アプリケーションへのアクセス権を制御するようにしてもよい。

【0057】リーダ/ライタ101とICチップ50との無線通信は、例えば電磁誘導の原理に基づいて実現される。図2には、電磁誘導に基づくリーダ/ライタ101とICチップ50との無線通信の仕組みを概念的に図解している。リーダ/ライタ101は、ループ・コイルで構成されたアンテナ $L_{RW}$ を備え、このアンテナ $L_{RW}$ に電流 $I_{RW}$ を流すことでその周辺に磁界を発生させる。一方、ICチップ50側では、電気的にはICチップ50の周辺にループ・コイル $L_c$ が形成されている。ICチップ50側のループ・コイル $L_c$ 端にはリーダ/ライタ101側のループ・アンテナ $L_c$ が発する磁界による誘導電圧が生じ、ループ・コイル $L_c$ 端に接続されたICチップ50の端子に入力される。

【0058】リーダ/ライタ101側のアンテナ $L_{RW}$ とICチップ50側のループ・コイル $L_c$ は、その結合度は互いの位置関係によって変わるが、系としては1個のトランスを形成していると捉えることができ、図3に示すようにモデル化することができる。

【0059】リーダ/ライタ101は、アンテナ $L_{RW}$ に流す電流 $I_{RW}$ を変調することで、ICカード上のループ・コイル $L_c$ に誘起される電圧 $V_0$ は変調を受け、そのことを利用してリーダ/ライタ101はICチップ50へのデータ送信を行うことができる。ここで言う送信データには、外部機器100側でユーザ入力された暗証番号やパスワードなどの、アプリケーションのアクセス権を

得るための暗証コードや、電子マネーや電子チケットなどのアプリケーションが提供する価値情報が含まれる。

【0060】また、ICチップ50は、リーダ/ライタ101へ返送するためのデータに応じてループ・コイル $L_c$ の端子間の負荷を変動させる機能 (Load Switching) を持つ。ループ・コイル $L_c$ の端子間の負荷が変動すると、リーダ/ライタ101側ではアンテナ端子間のインピーダンスが変化して、アンテナ $L_{RW}$ の通過電流 $I_{RW}$ や電圧 $V_{RW}$ の変動となって現れる。この変動分を復調することで、リーダ/ライタ101はICチップの返送データを受信することができる。外部機器100がICチップ50から受信するデータには、電子マネーや電子チケットなどのアプリケーションが提供する価値情報が含まれる。

【0061】図4には、本実施形態に係る携帯端末10に内蔵されるICチップ50内の機能構成を図解している。

【0062】同図に示すように、ICチップ50は、外部機器100側のリーダ/ライタ101と無線通信を行うアンテナが接続されるRF部51と、例えば購入済みチケット情報や銀行の預金者情報 (電子マネー) などのアプリケーション毎に割り当てられた記憶領域を持つメモリ52と、暗証コードの比較照合を行う照合部53と、有線インタフェース54と、これらの構成部品を統括的にコントロールする制御部55とからなる。

【0063】制御部55は、CPU (Central Processing Unit)、ROM (Read Only Memory)、RAM (Random Access Memory) などを一体化して構成されている。制御部55は、ROMに格納されたプログラム・コードを実行することによって、ICチップ50内の動作を制御する。また、制御部55は、有線インタフェース54を介して、携帯端末10側のコントローラ11と通信することができる。

【0064】メモリ52は、アプリケーション毎に領域が割り当てられている。図示の例では、メモリ52上には、アプリケーションA、アプリケーションB、アプリケーションCの各々に領域が割り当てられている。さらに、必要に応じて各アプリケーション毎に、本人確認又は認証処理用の暗証コードが設定されている。アプリケーションに割り当てられた領域内には、暗証コードを保存する暗証コード領域が含まれる。

【0065】なお、メモリ52は、半導体メモリの他、磁気ストライプなど、読み書き可能な記憶媒体であればよく、特定のデバイスには限定されない。

【0066】本実施形態においては、有線インタフェース54を通して送られてくる暗証コードを、照合部53において、各アプリケーションに割り当てられたメモリ領域に設定されている暗証コードと照合して、一致するされたメモリ領域に対するアクセスを許可する。アクセスが許可されたメモリ領域は、RF部51を介してリー

ダ/ライタ101から読み書きが可能となる。

【0067】有線インタフェース54を通して送られてくる暗証コードとは、要するに、携帯端末10上でユーザ入力された暗証コードのことである。すなわち、本実施形態によれば、ユーザは、操作が不慣れな外部機器100上のユーザ・インタフェースではなく、操作が手慣れた自分の携帯端末10上で暗証コードを入力操作して照合処理を受けることができる。

【0068】図5には、携帯端末10上のユーザ入力装置11から入力された暗証コードの照合処理によりメモリ52に割り当てられたアプリケーションのアクセス許可を行うための処理手順をフローチャートの形式で示している。以下、図5に示すフローチャートを参照しながら、アプリケーションのアクセス許可手続について説明する。

【0069】まず、ユーザは、携帯端末10上のユーザ入力装置11を使って、暗証コードを入力する (ステップS1)。

【0070】このように入力された暗証コードは、有線インタフェース52を介して、ICチップ50内の照合部53に転送される (ステップS2)。

【0071】次いで、照合部53は、メモリ52に割り当てられた各アプリケーションに対して設定されている暗証コードと、ユーザ入力装置12を介して入力された暗証コードとを比較照合する (ステップS3)。

【0072】そして、比較照合の結果、暗証コードが一致するアプリケーションに関するアクセス権がユーザに与えられる (ステップS4)。アクセス権が与えられたアプリケーションに割り当てられた記憶領域は、リーダ/ライタ101側からは無線通信によりアクセスすることが可能となる。

【0073】勿論、照合部53は、有線インタフェース54経由で受け取られた (すなわち携帯端末10上でユーザ入力された) 暗証コードを照合処理するだけでなく、RF部51経由で受信された (すなわち、外部機器100上でユーザ入力された) 暗証コードを照合処理することもできる。

【0074】また、アクセス許可後のリーダ/ライタ101との一連のトランザクションが終了したら、それを制御部55がこれを解釈して、有線インタフェース54を通して通知する。

【0075】あるいは、制御部55は、トランザクションの正常あるいは異常終了の後、有線インタフェース54からのコマンドを待つか、又は、携帯端末10本体の電源がOFFにされる (すなわち、リーダ/ライタ50側からの電波が途絶えて減勢される) のを待つ。この場合は、このICチップ50を搭載する携帯端末10側のコントローラ11が所定時間が経過した後に、ICチップ50に対して次のコマンドを送るか、又はICチップ50の電源をOFFにするなどの終了処理を行う。

【0076】図6には、外部機器50からの送信電波の検出結果によりアプリケーションのアクセス権を制御する処理手順をフローチャートの形式で示している。以下、このフローチャートに従って、アプリケーションのアクセス権制御について説明する。

【0077】RF部51経由で外部機器100と無線接続されている期間中、制御部55は、RF部51を介して電波を受信しているか否かを常にチェックしている（ステップS11）。

【0078】そして、電波が検出されなくなると、RF部51経由で無線接続されている外部機器100とICチップ50との一連のトランザクションが終了したと判断する（ステップS12）。

【0079】そして、制御部55は、外部機器100とのトランザクションの終了処理を行なう（ステップS13）。この結果、外部機器100に与えられていたアプリケーションへのアクセス権は消滅する。

【0080】この結果、使用後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末10を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【0081】また、図7には、ICチップ50からの送信コマンドに対する外部機器100からのレスポンスによりアプリケーションのアクセス権を制御する処理手順をフローチャートの形式で示している。以下、このフローチャートに従って、アプリケーションのアクセス権制御について説明する。

【0082】制御部55は、RF部51を介して外部機器100にコマンドを送信すると（ステップS21）、これに対するレスポンスが返されたか否かをチェックする（ステップS22）。

【0083】そして、コマンドを送信してから所定期間内にレスポンスが受信されなかった場合には（ステップS23）、ICチップ50と外部機器100との一連のトランザクションが正常又は異常終了したと判断して（ステップS24）、外部機器100とのトランザクションの終了処理を行なう（ステップS25）。

【0084】この結果、外部機器100との無線接続が断たれた後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【0085】また、ICチップ50は、有線インターフェース54経由で暗証コードが入力される前に、RF部41を通してリーダ／ライタ55との間で無線通信を行い、外部機器100との間でデータの送受信を行った後

に、制御部55がさらにデータの送受信を行う場合には暗証コードによる認証が必要であることを検出して、有線インターフェース54を通してその旨を携帯端末10側のコントローラ11に通知する。

【0086】図8には、ICチップ50がRF部51を介して外部機器100に無線接続されたことに応答して、携帯端末側に暗証コードの入力を促すための処理手順をフローチャートの形式で示している。

【0087】制御部55は、ICチップ50がRF部51を介して外部機器100に無線接続されたか否かを常にチェックする（ステップS31）。

【0088】そして、ICチップ50がRF部51経由で外部機器100に接続されて給電されると、制御部55は、有線インターフェース54経由で、携帯端末10のコントローラ11に対して、メモリ52にアクセスするために暗証コードの入力が必要である旨を通知する（ステップS32）。

【0089】携帯端末10側では、この通知に応答して、警告音を発したり、あるいは、表示装置12上にダイアログを出現させるなどして、ユーザに対して所望のアプリケーションを利用するための暗証コードの入力をプロンプトする。（ステップS33）。

【0090】したがって、ユーザは、携帯端末をリーダ／ライタなどの外部機器にかざしてアプリケーションを利用したいときに、暗証コードを入力する必要があるということを、確実に思い出すことができるので、ユーザの日常生活の各局面においてアプリケーションの使用が円滑化する。

【0091】図9には、本発明の他の実施形態に係る携帯端末10-2のハードウェア構成を模式的に示している。

【0092】図示の携帯端末10-2は、外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたICチップ50を搭載するとともに、携帯端末10内の動作を統括的に制御するコントローラ11と、ユーザが暗証番号やパスワードを始めとする各種の文字列やコマンドを入力するためのキー／ボタンなどからなるユーザ入力装置12と、処理結果を画面表示するための液晶ディスプレイ（LCD：Liquid Crystal Display）などの表示装置13を備えている。もちろん、携帯端末10-2としての本来の機能を実現するために、図示する以外の周辺装置や回路コンポーネントを備えていてもよい。

【0093】ICチップ50は、外部機器100と無線接続するための無線インターフェース14と、携帯端末10側のコントローラ11と有線接続するための有線インターフェース15を備えている。無線インターフェース14に関しては、例えば、ISO 7816で定義された接触インターフェース規格、又は、ISO 14443で定義された無線インターフェース規格を使用する

ことができる(同上)。

【0094】ICチップ50は、例えば、非接触ICカードの技術が適用されており、無線インターフェース経由で受信される外部機器100からの電波によって駆動する。言い換えれば、外部機器100に携帯端末10をかざしていない状態では、外部機器100からの電波が届かないので、ICチップ50は減勢されて、ICチップ50内部へのアクセス権は消失する。

【0095】また、ICチップ50は、比較的大容量のメモリ領域を備えている。このようなメモリ領域は、微細化技術などによりもたらされる。メモリ領域は、半導体メモリや磁気ストライプ、あるいは読み書き可能なその他の記憶媒体で構成される。このメモリ領域上には、1以上のアプリケーションが割り当てられている。ここで言うアプリケーションの例としては、電子マネーや電子チケットを始めとする価値情報を挙げることができる。

【0096】この種の価値情報を無断使用や盗用から保護するために、各アプリケーション毎に暗証番号やパスワードなどの暗証コードによってアクセス権が制御されている。例えば、無線インターフェース14や有線インターフェース15を介して入力された暗証コードと各アプリケーションが持つ暗証コードとを比較照合して、一致するアプリケーションについてのアクセス権が与えられる。

【0097】携帯端末10-2は、図1で示された携帯端末内のコントローラ11内に暗証コード記憶領域を備えたものである。したがって、あらかじめコントローラ11内のプログラムに対応した暗証コードをこの暗証コード記憶領域に記憶しておくことによって、呼び出されたプログラムに応じて対応する暗証コードを有線インターフェース経由でICチップ50側に送出することができる。したがって、ユーザは、ICチップ50内に格納された同じアプリケーションを使用するために、暗証コードを逐次入力する必要がなくなり、機器の操作性が向上する。

【0098】図10には、プログラムの起動により暗証コードの入力を省略するための処理手順をフローチャートの形式で示している。

【0099】まず、アプリケーション毎にあらかじめ暗証コードを登録する(ステップS41)。登録された暗証コードは、コントローラ55内の所定の暗証番号記憶領域に格納される。

【0100】そして、ユーザは、アプリケーションを使用したい局面においては、例えば、表示装置13上に表示されたメニューリスト(図示しない)を介して、所望のプログラムを選択する(ステップS42)。

【0101】この結果、コントローラ11は、選択されたプログラムを起動する(ステップS43)。

【0102】そして、コントローラ11は、この起動さ

れた起動されたプログラムに応じて該当するアプリケーションに対応する暗証コードを暗証コード記憶領域から読み出して、有線インターフェース15経由でICチップ50に送出する(ステップS44)。

【0103】この結果、ICチップ内では、メモリ領域に割り当てられた各アプリケーションに対して設定されている暗証コードと、有線インターフェース15経由で入力された暗証コードとを比較照合する(ステップS45)。

【0104】そして、比較照合の結果、暗証コードが一致するアプリケーションに関するアクセス権がユーザに与えられる(ステップS46)。アクセス権が与えられたアプリケーションに割り当てられた記憶領域は、リーダー/ライター101が無線通信によりアクセスすることが可能となる。

【0105】このような場合、ユーザがディスプレイに表示されたメニュー画面などを介して所望のプログラムを選択して、携帯端末上で該当するプログラムが呼び出される。そして、起動されたプログラムに回答して、対応するアプリケーションについての暗証コードが前記有線インターフェース経由でICチップに入力されてアクセス権を与えることができる。したがって、ユーザは、使用したいアプリケーションの暗証コードを入力する作業を省略することができるので、機器操作性が向上する。

【0106】[追補]以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。

【0107】本明細書中では、本発明に係るICチップが携帯電話機やPDAなどの携帯端末に内蔵して使用される場合を例にとって説明してきたが、本発明の要旨はこれに限定されない。例えば、スタンドアロンのICカードとして使用する場合や他の機器に内蔵してICチップを使用する場合においても、同様に本発明の効果を奏することができる。

【0108】要するに、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参照すべきである。

【0109】

【発明の効果】以上詳記したように、本発明によれば、外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたICチップを搭載した優れた携帯端末及びその制御方法、並びに、メモリ機能を備えた優れたICカードを提供することができる。

【0110】また、本発明によれば、ICチップ上のメモリ領域に1以上のアプリケーションが割り当てることができる、優れた携帯端末及びその制御方法、並びに、

メモリ領域に1以上のアプリケーションが割り当てた優れたICカードを提供することができる。

【0111】また、本発明によれば、ICチップ上のメモリ領域に割り当てられた各アプリケーション毎にアクセス権を制御することができる、優れた携帯端末及びその制御方法、並びに、メモリ領域に割り当てられた各アプリケーション毎にアクセス権を制御することができる優れたICカードを提供することができる。

【0112】本発明によれば、例えば携帯端末上に内蔵したICチップを銀行用カードとして使用する場合には、使用者にとって使い慣れた携帯端末側で暗証番号を入力することによって、本人確認又は認証処理を受けることができる。この結果、不慣れな銀行のATM端末に対する操作を最小限にすることができる。

【0113】また、本発明によれば、例えば銀行内のATM端末に向かって携帯端末をかざすことによって、ATM端末側から携帯端末に対して適切な暗証番号の入力を促すことができる。

【0114】また、本発明によれば、携帯端末内においてプログラムと暗証コードを結び付けておくことによって、例えば、ある銀行の残高表示プログラムが呼び出されたとき、自動的に暗証番号が呼び出される。

#### 【図面の簡単な説明】

【図1】本発明の一実施形態に係る携帯端末10のハードウェア構成を模式的に示した図である。

【図2】電磁誘導に基づくリーダ/ライタ101とICチップ50との無線通信の仕組みを概念的に示した図である。

【図3】リーダ/ライタ101とICチップ50からなる系を1個のトランスとして捉えてモデル化した図である。

【図4】本実施形態に係る携帯端末10に内蔵されるICチップ50内の機能構成を示した図である。

【図5】携帯端末10上のユーザ入力装置11から入力

された暗証コードの照合処理によりメモリ52に割り当てられたアプリケーションのアクセス許可を行うための処理手順を示したフローチャートである。

【図6】外部機器50からの送信電波の検出結果によりアプリケーションのアクセス権を制御する処理手順を示したフローチャートである。

【図7】ICチップ50からの送信コマンドに対する外部機器100からのレスポンスによりアプリケーションのアクセス権を制御する処理手順を示したフローチャートである。

【図8】ICチップ50がRF部51を介して外部機器100に無線接続されたことに応答して、携帯端末側に暗証コードの入力を促すための処理手順を示したフローチャートである。

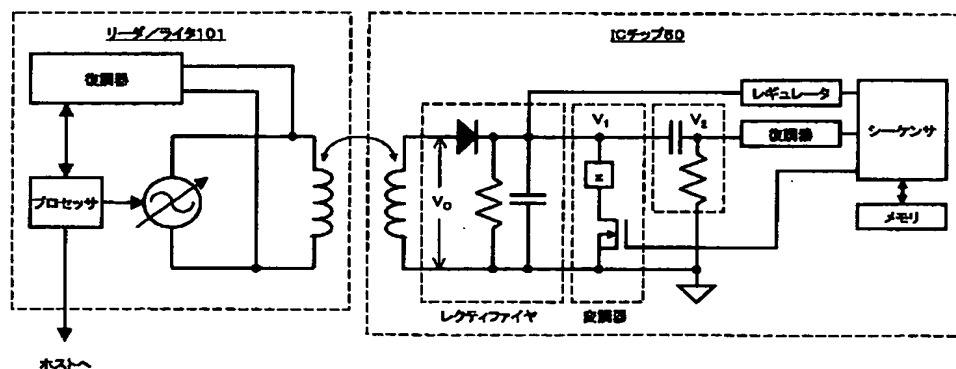
【図9】本発明の他の実施形態に係る携帯端末10-2のハードウェア構成を模式的に示した図である。

【図10】プログラムの起動により暗証コードの入力を省略するための処理手順を示したフローチャートである。

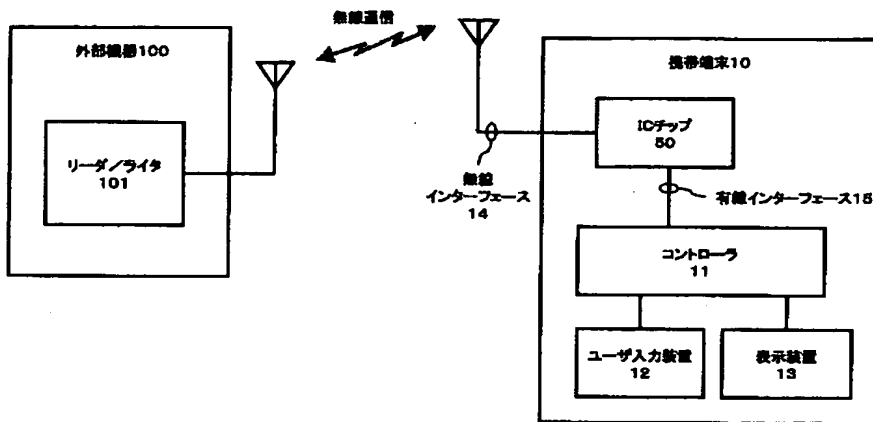
#### 【符号の説明】

- 10…携帯端末
- 11…コントローラ
- 12…ユーザ入力装置
- 13…表示装置
- 14…無線インターフェース
- 15…有線インターフェース
- 50…ICチップ
- 51…RF部
- 52…メモリ
- 53…照合部
- 54…有線インターフェース
- 55…制御部
- 100…外部機器
- 101…リーダ/ライタ

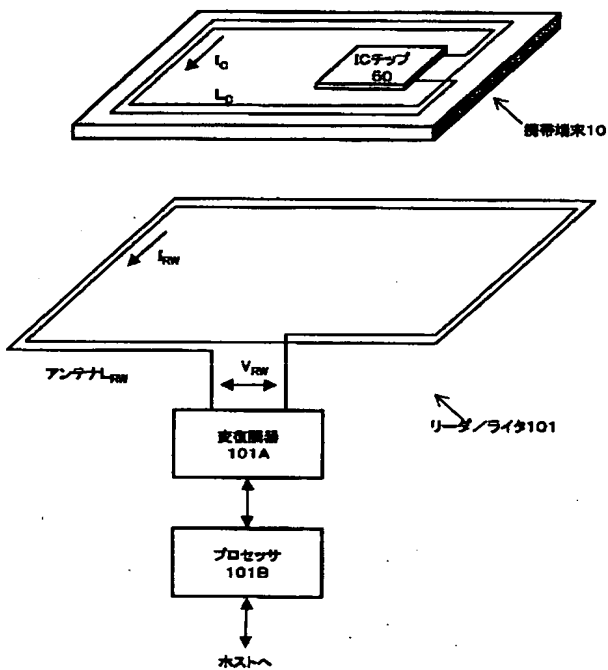
【図3】



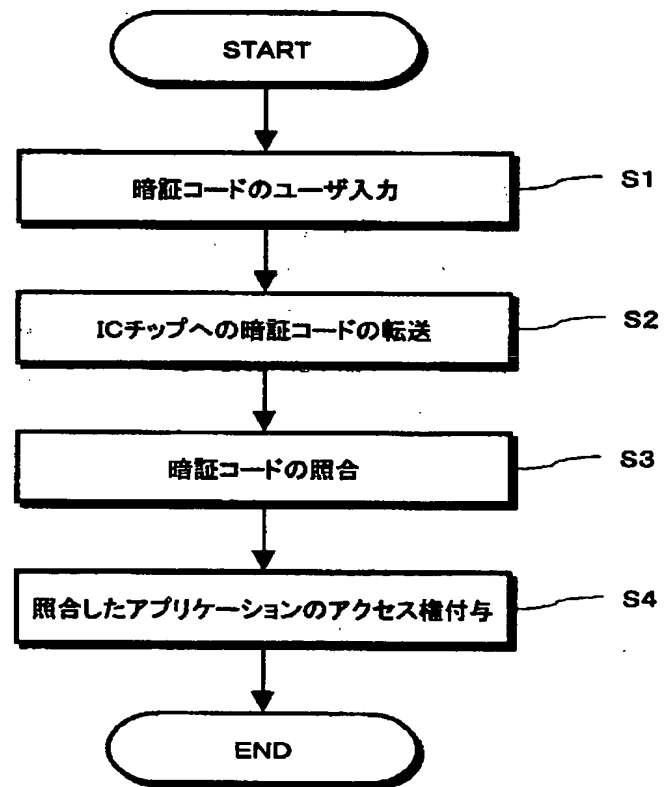
【図1】



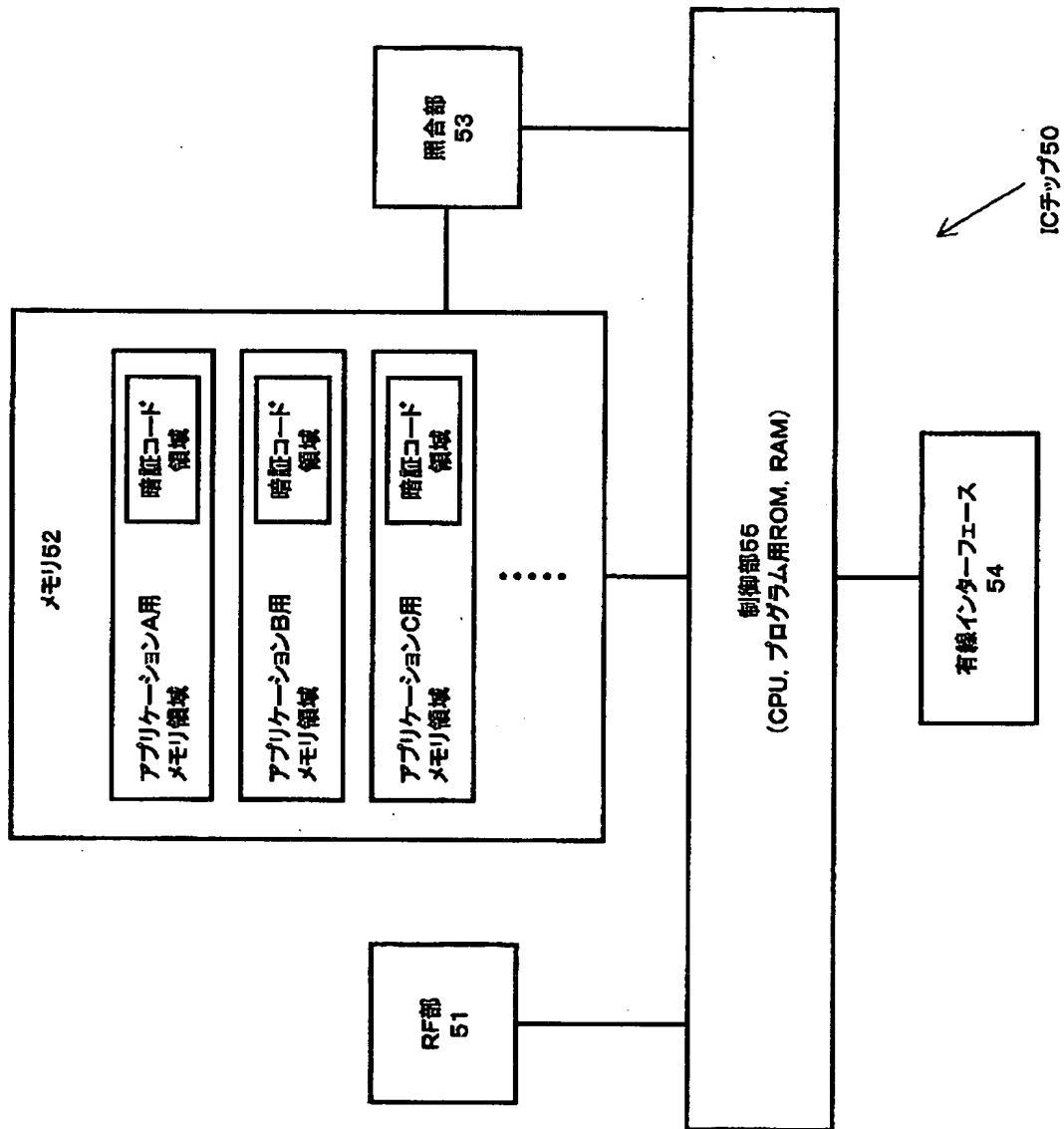
【図2】



【図5】

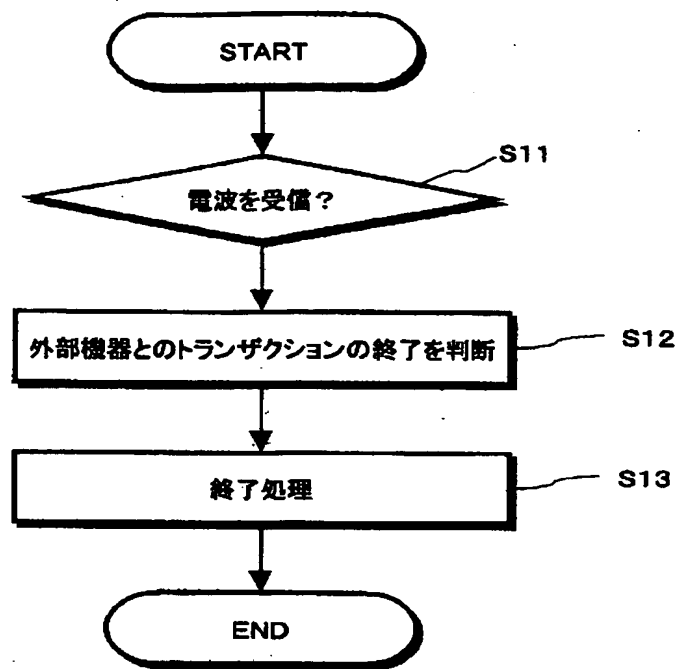


【図4】

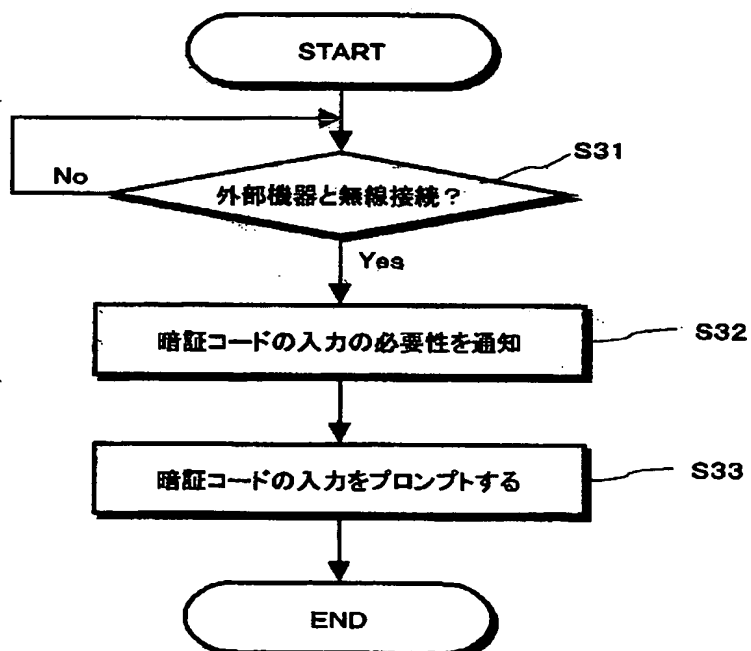




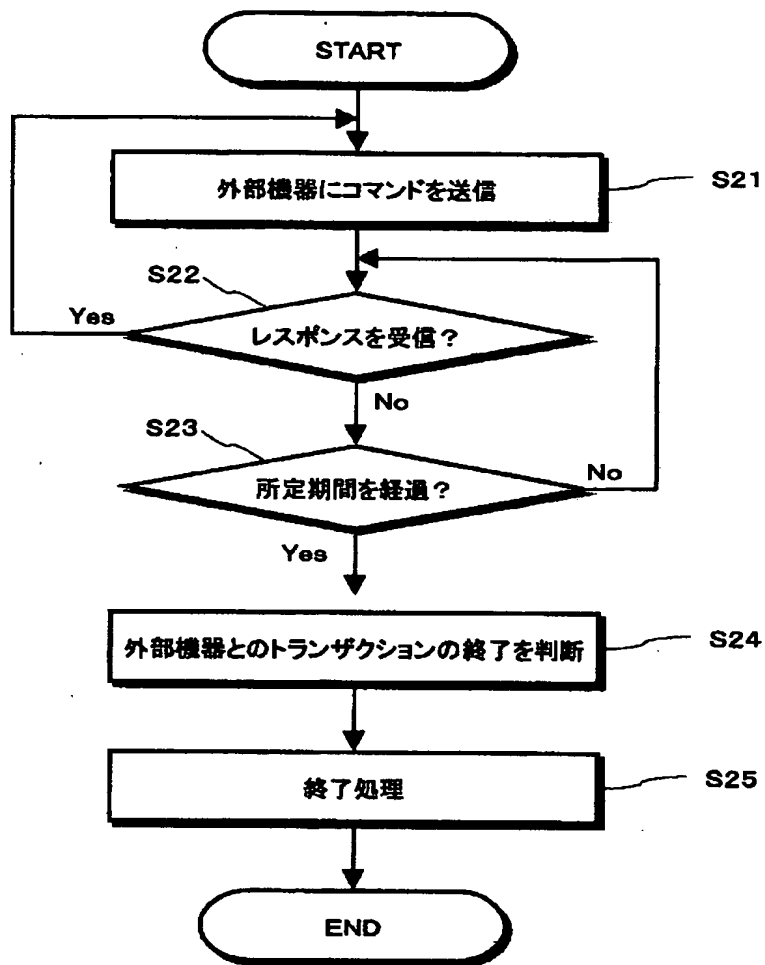
【図6】



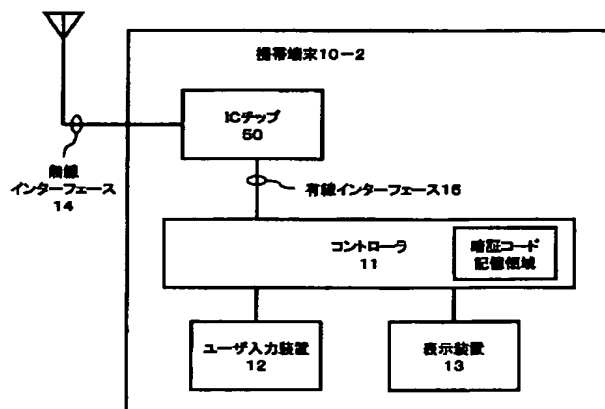
【図8】



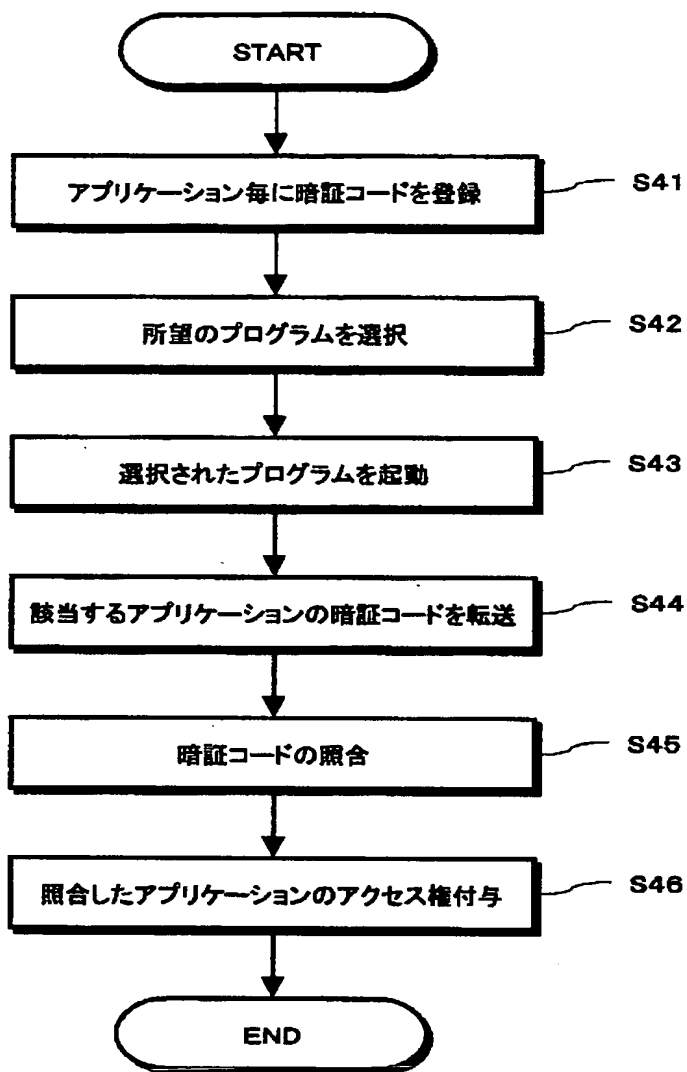
【図7】



【図9】



【図10】



フロントページの続き

Fターム(参考) 2C005 MB08 NA08 NA09 SA02 SA05  
SA12 SA22 SA25 TA21 TA22  
5B017 AA03 BA05 CA14 CA15  
5B035 AA06 AA13 BB09 BC00 CA12  
CA23 CA38  
5B082 EA12